REMARKS

Claims 1-187 and 189-193 are currently pending. Applicants respectfully request reconsideration of the above-identified application in light of the above amendment and the following remarks.

Claim 1 has been amended to recite the step of "encrypting data contained within the digital rights management container via the computer program resident on the personal computer...." to further define Applicants' invention. Support for this amendment is found throughout the Specification and drawings, as filed, for example at page 14, lines 16-20, page 10, line 18- page 11, line 2.

Independent claim 1 additionally recites, and independent claims 19, 28, 46, 55, 73, 82, 100, 109-111, 113, 115-117, 119 and 189 recite that "a computer program resident on a personal computer," "without the use of a secure network," is used to either assign security indicia when sending or enter security indicia when receiving money in the manner defined in each claim, respectively. Independent claims 1, 19, 28, 46, 55, 73, 82, 100, 109-111, 113, 115-117, 119 and 189 recite that money is either sent or received via "an insecure network," in the manner defined in each claim, respectively.

Moreover, Independent claims 1, 19, 28, 46, 55, 73, 82, 100, 109-111, 113, 115-117, 119, and 189 further recite a "sender-defined security attribute." Independent claims 1, 28, 55, 82, 109, 111, 115, 117 and 189 recite, "wherein the at least one sender-defined security attribute is defined at the time of an electronic fund transfer." Independent claims 19, 73 and 110, recite, "wherein the at least one sender-defined security attribute is defined at the time a sender sends the digital rights management container," and claims 46, 100, 113, 116 and 119

recite, "wherein the at least one sender-defined security attribute is defined at the time a sender sends the secure file."

Claim Rejections Under 35 U.S.C. §103

2. Claims 1-15, 19-27, 55-61, 73-81, 100-112, 121, 122, 126, 128, 129, 130, 140-149, 155-159, 162-164, 172-174, 177-179, 180-182, 189, and 190-193 have been rejected under 35 U.S.C. §103(a) as being anticipated by U.S. Patent No. 5, 371,797 to Bocinsky ("Bocinsky") in view of U.S. Patent No. 6, 047,887 to Rosen ("Rosen"). Applicants respectfully traverse this rejection.

"To establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art." (MPEP § 2143.03 (citing In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974))).

As set forth above, independent claims 1, 19, 28, 46, 55, 73, 82, 100, 109-111, 113, 115-117, 119 and 189 recite that "a computer program resident on a personal computer," "without the use of a secure network," is used to either assign security indicia when sending or enter security indicia when receiving money in the manner defined in each claim, respectively, and that money is either sent or received via "an insecure network," in the manner defined in each claim, respectively.

Additionally, independent Claim 1 has been amended to recite "encrypting data contained within the digital rights management container via the computer program resident on the personal computer...."

Independent claims 1, 19, 28, 46, 55, 73, 82, 100, 109-111, 113, 115-117, 119, and 189 also recite a "sender-defined security attribute." Independent claims 1, 28, 55, 82, 109,

111, 115, 117 and 189 recite, "wherein the at least one sender-defined security attribute is defined at the time of an electronic fund transfer" (emphasis added); independent claims 19, 73 and 110, recite, "wherein the at least one sender-defined security attribute is defined at the time a sender sends the digital rights management container" (emphasis added); and claims 46, 100, 113, 116 and 119 recite, "wherein the at least one sender-defined security attribute is defined at the time a sender sends the secure file" (emphasis added).

In contrast, Applicants maintain that Bocinsky describes a system and apparatus in which an encrypted PIN is defined by a computer on a secure network, *not* a personal computer utilizing an insecure network. Though the Office Action maintains that "the process of providing the access code, which is unmasked with the second portion to recreate the original full encrypted PIN is readable as [a] security attribute that is defined at the time of the fund transfer." See Office Action at page 3, lines 4-12, this "concatenation" described by Bocinsky is still carried out by a computer and not by a user. Thus, the initial encrypted PIN is created by and separated by the computer (before the time of a fund transfer), and then recreated (by the computer) to provide customer access.

The January 7, 2005 Office Action states, "Bocinsky fails to explicitly disclose that the security of the electronic funds is without the use of a secure network," continuing, "However, Rosen discloses a certification agency 28 for providing a process that certifies the validity of a money module for a certain period of time by issuing a certificate instead of a secure network." The Office Action argues, "It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the teaching of Bocinsky by including the limitation detailed above as taught by Rosen because this would determine the validity of an

electronic fund transfer based on a user PIN or ID or Password." See January 7, 2005 Office Action at page 3.

Thus, the Office Action, as with prior Office Actions argues that every claimed element, with the exception of an "insecure network" is taught by Bocinsky. The Office Action also argues that the alleged certification agency and issuance of a certificate, in lieu of use of a secure network, in combination with the system and apparatus of Bocinsky renders obvious Applicants' claimed invention.

However, Applicants respectfully submit that Bocinsky describes a system and apparatus in which an encrypted PIN is defined by a computer prior to the time of a transaction, during a separate, preceding event. Additionally, this encrypted PIN is created through the use of a secure network.

Bocinsky describes a system and method involving at least two main stages. In the first stage, a "secure transaction processor" (Bocinsky, Abstract, line 8), such as a secure point of sale terminal (Bocinsky, col. 4, line 24), is utilized to encrypt a PIN. The PIN is encrypted using a key that is "acquired from either a specific request to, or monitoring data passing from a conventional network security transaction processor" (Bocinsky, Abstract, lines 12-15). This encrypted PIN is broken into two parts, one is provided to the user, the other is stored in the system. Figure 3 of Bocinsky illustrates the parsing of the encryption key (62) into two segments, storing of an N-M character length segment (65), and transmission of an M-character length segment to the customer (68). This first stage allows for the second stage to occur securely. More specifically, the M-character length segment is later used in the second stage by the customer when using an insecure network to perform a transaction.

In the second stage, an insecure network (such as a telephone system), is used to perform a financial transaction using a portion of the encrypted PIN (M-character length segment) generated during the first stage. This process is illustrated in Figure 4 of Bocinsky. The only action required on the part of the customer, at the time of performing a transaction, is inputting pre-determined values into the system ("TSAN" in 75, "M-char" in 77). The system then "concatenates" the provided M-character length segment to the N-M-character length segment to reconstitute the N-character length segment. Nothing during the transaction is being "defined," as required by independent claims 1, 19, 28, 46, 55, 73, 82, 100, 109-111, 113, 115-117, 119, and 189. Rather, these values have all been pre-determined in one way or another. If anything in Bocinsky, is "defined," the definition occurs in the first stage, *not* during this second stage during which the actual transaction is occurring.

The Office Action argues:

> ...the process of providing the access code, which is unmasked with second portion to recreate the original full encrypted PIN is readable [as] a security attribute that is defined at the time of the fund transfer...

and that

> ...the security attribute is interpreted as the customer security identification such as PIN number that also includes encryption key, password and so....

See Office Action at pages 2-3.

However, Applicants respectfully submit that the alleged "definition" does not occur at the time of a fund transfer, and that the recreation of the original full encrypted PIN does not constitute a "definition." In contrast, it is indeed, only a "recreation." The encrypted PIN had been previously "defined" in the above-described first stage, and during the transaction is merely being "reconstituted" (or recreated). Further, as stated above, the "concatenation" step of

Bocinsky is accomplished by computer, and not by the user. The Office Action does not allege that Rosen remedies this deficiency of Bocinsky.

While the customer in Bocinsky "provides" an access code, the customer does not "define" the access code at the time of the transaction, as required by independent claims 1, 19, 28, 46, 55, 73, 82, 100, 109-111, 113, 115-117, 119, and 189.

Even if the access code (Bocinsky, Abstract, line 19) were considered to be "defined by the user," which Applicants maintain it is not, such definition would occur in a first stage, prior to any actual financial transaction. Bocinsky states that the action occurring during the transaction is "concatenation."

The access code is simply being re-united with the other portion of the encrypted PIN. No "definition" occurs at this stage, only what may be considered a reconstitution of a *previously* "defined," encrypted PIN. The Office Action does not allege that Rosen remedies any of these foregoing deficiencies of Bocinsky.

While the claimed invention, as defined by claims 1, 19, 28, 46, 55, 73, 82, 100, 109-111, 113, 115-117, 119, and 189, may be carried out completely over insecure networks, such as the internet, Bocinsky requires the use of a secure network for the creation of an encrypted PIN. Thus, even if Bocinsky taught or suggested every other feature of the claimed invention (which it does not), the benefits of the present invention, as claimed, could not be fully realized through the practice of Bocinsky. Traditional networks such as that contemplated by Bocinsky allow for anyone with an encryption key to use the data and take it anywhere he or she wishes, while the claimed invention protects the data even in an insecure network.

The Office Action alleges that the issuance of a certificate by Rosen, instead of use of a secure network, renders obvious this aspect of the claimed invention, and thus, in

combination with Bocinsky, the invention as a whole. For the reasons set forth above, Bocinsky is deficient in a number of respects in teaching or suggesting the claimed subject matter, which the Office Action does not allege are remedied by Rosen.

Regarding the aspect of an insecure network versus the "certificate," of Rosen identified by the Office Action- the claimed subject matter does not utilize such a "certificate" as alleged by the Office Action. Rather, the invention as claimed, provides security through an object itself (e.g. the "digital rights management container"), and not through the use of a network, as described by Bocinsky or another element, such as the "certificate" of Rosen, alleged by the Office Action. In Bocinsky, the network is used in and relied on in both creating the encrypted PIN and in using the encrypted PIN to perform a transaction. Regarding Rosen, the Office Action argues that a secondary "certificate" "certifies the validity of a money module." See Office Action at page 3. In the present invention, as claimed, while a "network" such as the internet may be used for transmission in the present invention, permission to access the object is not provided by the network or a "certificate", but by the object (e.g. the "digital rights management container"), itself.

For at least the foregoing reasons, independent claims 1, 19, 28, 46, 55, 73, 82, 100, 109-111, 113, 115-117, 119, and 189, and claims depending from these claims, define patentable subject matter over Bocinsky and Rosen, considered alone or in combination. Withdrawal of the rejection applied to claims 1-15, 19-27, 55-61, 73-81, 100-112, 121, 122, 126, 128, 129, 130, 140-149, 155-159, 162-164, 172-174, 177-179, 180-182, 189, and 190-193 under 35 U.S.C. §103(a) as being unpatentable over Bocinsky in view of Rosen is respectfully requested.

3. Claims 16-18, 28-54, 62-72, 82-99, 113-120, 123, 124, 125, 127, 131-139, 150-154, 160, 161, 165-169, 170, 171, 175, 176, 183, 186, 187 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Bocinsky in view of Rosen. Applicants respectfully traverse this rejection.

"To establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art." (MPEP § 2143.03 (citing In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974))).

For at least the reasons set forth above, Bocinsky and Rosen, alone or in combination, do not teach or suggest each and every element of independent claims 1, 19, 28, 46, 55, 73, 82, 100, 109-111, 113, 115-117, 119, and 189, and thus these claims define patentable subject matter over Bocinsky and Rosen, considered alone or in combination. Each of the rejected claims depends from one of these independent claims, and therefore also defines patentable subject matter over Bocinsky and Rosen, considered alone or in combination.

Withdrawal of the rejection applied to claims 16-18, 28-54, 62-72, 82-99, 113-120, 123, 124, 125, 127, 131-139, 150-154, 160, 161, 165-169, 170, 171, 175, 176 and 183, under 35 U.S.C. §103(a), as being unpatentable over Bocinsky in view of Rosen, is respectfully requested.

CONCLUSION

In light of the foregoing, Applicants believe that all claims, as currently presented, are patentable, and that this application is in condition for allowance.

In the event that a telephonic or personal interview would facilitate the examination of this application in any way, Applicant and his Attorneys hereby invite the Examiner to contact the undersigned at the number provided.

Respectfully submitted,
MORGAN & FINNEGAN, L.L.P.

Dated: April 7, 2005

Michael J. Pollack
Registration No. 53,475

Correspondence Address:
MORGAN & FINNEGAN, L.L.P.
3 World Financial Center
New York, NY 10281-2101
(212) 415-8700 Telephone
(212) 415-8701 Facsimile